The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/20/2020

SUBJECT:
A Vulnerability with Cisco Small Business, Smart, and Managed Switches Could Allow for Denial of Service

OVERVIEW:
A vulnerability has been discovered in Cisco Small Business, Smart, and Managed Switches, which could allow for a denial-of-service condition. These switches are designed with easy to use web management interfaces and flexible plug and play design. Successful exploitation of this vulnerability could allow an attacker to cause the switches management CLI to stop responding.

THREAT INTELLIGENCE:
There are no reports of the vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- 250 Series Smart Switches
- 350 Series Managed Switches
- 350X Series Stackable Managed Switches
- 550X Series Stackable Managed Switches
- Small Business 200 Series Smart Switches
- Small Business 300 Series Managed Switches
- Small Business 500 Series Stackable Switches

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

A vulnerability has been discovered in Cisco Small Business, Smart, and Managed Switches which could allow for a denial-of-service condition when the switch processes a specially crafted IPv6 address. The vulnerability occurs due to insufficient validation of incoming IPv6 traffic. An unauthenticated remote attacker could exploit this vulnerability by sending a crafted IPv6 packet through an affected device. The vulnerability does not affect IPv4 traffic and there is no workaround for the vulnerability. Successful exploitation of this vulnerability could allow an attacker to cause the switches management CLI to stop responding.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Cisco to vulnerable devices immediately after appropriate testing.
- Deploy network intrusion detection systems to monitor network traffic to affected devices.

REFERENCES:
Cisco:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbss-ipv6-dos-tsgqbffW

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3496